2

3

4

5

6

7

8

9

1

2

3

1

2

3

1

2

3

RPS9-2001-0022 PATENT

## WHAT IS CLAIMED IS:

1	A method	comprising	the	stens	of:
1.	A memou	Comprising	uic	oupo	$\mathbf{o}_{\mathbf{r}}$

receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA);

creating a public/private key pair and a third certificate in response to the receiving step; and

sending the public/private key pair and the third certificate to the customer over the network.

- 2. The method as recited in claim 1, wherein after the sending step, the customer is capable of using the public/private key pair and the third certificate to make purchases over the network.
- 3. The method as recited in claim 1, wherein the TPM identity is a public/private key pair created as a result of a command by the customer input into the computer system.
- 4. The method as recited in claim 1, wherein the second certificate is created by the Certification Authority in response to receiving a third certificate signed by a manufacturer of the TPM and a public key of the TPM identity.

1	5.	The method as recited in claim 4, wherein the third certificate is associated with
2	an end	orsement key of the TPM.
1	6.	The method as recited in claim 1, wherein the network is the Internet.
2	7.	A method comprising the steps of:
3		creating a TPM identity at a customer's computer system;
4		the customer's computer system obtaining a first certificate from a first server
5	suppor	rting a CA over a network;
6		the customer's computer system creating a non-migratable key; and
7		transferring an application for a credit card authorization, the TPM identity, the
8	non-m	nigratable key, and the first certificate from the customer's computer system to a
9	secon	d server supporting a credit card company.
1	8.	The method as recited in claim 7, further comprising the steps of:
2		the second server supporting the credit card company creating a public/private
3	key pa	air and a second certificate in response to the transferring step; and
4		transferring the public/private key pair and the second certificate from the second

server supporting the credit card company to the customer's computer system.

2

3

4

1

2

3

4

5

6

1

1

2

9.	The	method	as	recited	in	claim	8,	wherein	the	step	of	transferring	the
publica	/priva	te key pa	ir a	nd the se	cor	nd certif	fica	te from th	e sec	cond s	serv	er supporting	g the
credit	card c	ompany	to t	he custo	mer	's comp	ute	r system i	s pei	form	ed u	ising a traditi	onal
mail se	ervice	<u>.</u>											

- 10. The method as recited in claim 8, wherein the step of transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system is performed using the network.
- 11. The method as recited in claim 8, further comprising the step of:
  a customer using the public/private key pair and the second certificate for commercial transactions over the network.
- 12. The method as recited in claim 11, wherein the network is the Internet.
- 13. The method as recited in claim 7, wherein the creating step further comprises creating a public/private key pair.

RPS9-2001-0022 PATENT

1	14. The method as recited in claim 13, wherein the step of the customer's computer
2	system obtaining the first certificate from the first server supporting the CA over the
3	network further comprises the steps of:
4	transferring from the customer's computer system to the first server supporting
5	the CA a public portion of the public/private key pair created when the TPM identity is
6	created and a third certificate associated with an endorsement key of the TPM;
7	the CA checking an authenticity of the third certificate;
8	the CA creating a fourth certificate for the TPM identity;
9	the CA encrypting the fourth certificate;
10	the CA bundling the encrypted fourth certificate with the public portion of the
11	public/private key pair created when the TPM identity is created to create a first bundle;
12	and
13	the CA encrypting the first bundle with a public key of the third certificate to
14	create a second bundle.
1	15. The method as recited in claim 14, wherein the step of transferring the
2	public/private key pair and the second certificate from the second server supporting the
3	credit card company to the customer's computer system further comprises the steps of:
4	the TPM decrypting the second bundle with a private portion of the third
5	certificate producing the first bundle; and
6	the TPM decrypting the first bundle with a private portion of the public/private
7	key pair created when the TPM identity is created.

16. A computer program product adaptable for storage on a computer readable medium, comprising the program steps of:

receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA);

creating a public/private key pair and a third certificate in response to the receiving step; and

sending the public/private key pair and the third certificate to the customer over the network.

- 17. The computer program product as recited in claim 16, wherein after the sending step, the customer is capable of using the public/private key pair and the third certificate to make purchases over the network.
- 18. The computer program product as recited in claim 16, wherein the TPM identity is a public/private key pair created as a result of a command by the customer input into the computer system.
- 19. The computer program product as recited in claim 16, wherein the second certificate is created by the Certification Authority in response to receiving a third certificate signed by a manufacturer of the TPM and a public key of the TPM identity.

RPS9-2001-0022

4

1	20.	The computer program product as recited in claim 19, wherein the third certificate					
2	is asso	is associated with an endorsement key of the TPM.					
3	21.	A computer program product adaptable for storage on a computer readable					
4	mediu	m, comprising the program steps of:					
5		creating a TPM identity;					
6		obtaining a first certificate from a CA;					
7		creating a non-migratable key;					
8		contacting a web site supporting a credit card company;					
9		sending to the web site an application for a credit card authorization, the TPM					
10	identit	y, the first certificate, and the non-migratable key; and					
11		receiving from the web site a public/private key pair and a second certificate					
12	enabli	ng the credit card authorization.					
1	22.	The computer program product as recited in claim 21, further comprising the					
2	progra	am step of:					
3		conducting a commercial transaction over the Internet using the credit card					

authorization as enabled by the public/private key pair and the second certificate.

- 1 23. The computer program product as recited in claim 21, wherein the non-migratable 2 key is a signing key.
- 1 24. The computer program product as recited in claim 21, wherein the non-migratable
- 2 key is a storage key.

1	25.	A system comprising:
2		a server supporting a web site of a credit card company;
3		a customer computer including a TPM;
4		a network linked to the server and the customer computer;
5		first software stored in memory in the customer computer for requesting the TPM
6	to crea	ate a TPM identity;
7		second software stored in memory in the customer computer for obtaining a first
8	certifi	cate over the network from a CA;
9		third software stored in memory in the customer computer for creating a
10	non-n	nigratable key;
11		fourth software stored in memory in the customer computer for browsing the web
12	site of	the credit card company over the network;
13		fifth software stored in memory in the customer computer for sending an
14	applic	cation for a credit card authorization to the web site of the credit card company over
15	the ne	etwork;
16		sixth software stored in memory in the customer computer for sending to the web
17	site o	f the credit card company over the network the TPM identity, the first certificate,
18	and th	ne non-migratable key;
19		the web site of the credit card company creating a public/private key pair and a
20	secon	d certificate; and
21		the web site of the credit card company sending the public/private key pair and

the second certificate over the network to the customer computer.